UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,423	03/29/2001	Michael S. Ripley	42390P10855	9405

8791 7590 06/15/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/823,423	RIPLEY ET AL.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-26 remain for examination. The correspondence filed 3/17/05 amended claims 1, 11, and 18.

Response to Arguments

2. Applicant's arguments filed 3/17/05 have been fully considered but they are not persuasive.

Applicant argues, "Neither Lotspiech nor Utsumi suggests or teaches receiving the nonce over the data bus and sending the encrypted data over the same data bus.". Examiner disagrees with this contention. Note that the encryption module disclosed in Lotspiech contains a dedicated processor for encryption in communication with a computer (col. 3, lines 44-57). In addition, Lotspiech also discloses that the encryption module is capable of both reading and writing to the flash memory device (col. 5, line 66 – col. 6, line 11), which at the minimum suggests that the invention is capable of communicating such information over the same bus.

Applicant further argues, "*Further, the combination of Utsumi with Lotspiech is inappropriate as this combination would alter the principle of operation of the primary reference Lotspiech. The Examiner admits in the above-identified office action that Lotspiech does not disclose an encryption subsystem housed within a storage device. Rather, the encryption module in Lotspiech is housed within a computer kiosk responsible for updating the media m, generating an encryption key, and controlling the check-ins and check-outs of digitized music rental (see Abstract). Removing the encryption module from the kiosk to a storage device as taught by Utsumi would make it impossible for a user to rent music from the kiosk because the digitized music checked out from the kiosk would not be encrypted. Thus, the*

proposed combination of Utsumi with the primary reference of Lotspiech is inappropriate." Examiner disagrees with this contention. Note that the kiosk disclosed by Lotspiech contains a storage device (element 16 of Figure 1); thus the proposed modification does not actually remove the encryption elements away from the kiosk, and the principle of operation of the prior art is not altered. Furthermore, Utsumi provides motivation for relocating the encryption component, in that it better allows for the protection of copyrighted materials (paragraphs 0020-0021).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-9, 11-14, 16, 18-21, 23-24, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech (U.S. Patent 6,748,539), and further in view of Utsumi et al. (U.S. Pre-Grant Patent Application 2001/0032088).

Referring to Claim 1:

Lotspiech discloses a system comprising:

a number generator to generate a nonce (col 5, lines 20-30); and

an encryption subsystem to encrypt data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting

the encrypted data via a data bus (col 3, lines 10-16), wherein said encryption bus key is derived based on [1] a portion of the key distribution data block, [2] a device key assigned to said encryption subsystem and [3]the nonce received over the data bus from the number generator (col 3, lines 10-20; col 4, line 65-col 5, line 10).

Lotspiech does not disclose that the encryption subsystem is housed within a storage device. However, Utsumi discloses an encryption subsystem housed in a storage device (Utsumi, elements 20 and 22 of Figure 1, and paragraph 0034). Utsumi and Lotspiech are analogous art as they both pertain to the field of digital copyright protection. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include an encryption subsystem inside a drive such as the one contained within the invention disclosed by Lotspiech. The motivation for doing so would be to minimize the number of components that have access to the encrypted information, thus more reliably protecting digital contents (Utsumi, paragraph 0020).

Referring to Claim 11:

Lotspiech discloses a method comprising:

a storage device reading a key distribution data block from a storage medium (col 4, line 65-col 5, line 10);

the storage device processing at least a portion of said key distribution data block using least one device key to compute a media key (col 5, lines 1-10);

the storage device fetching a nonce received over a data bus from a number generator (col 5, lines 1-6, 20-25);

the storage device combining said nonce with said media key using a one-way function to generate a bus key (col 5, lines 5-10);

encrypting data read from the storage medium using the generated bus key (col. 5, lines 5-10); and

the storage device transmitting the encrypted data over a data bus to a host device (col 5, lines 5-20).

Lottspiech does not explicitly disclose that the storage device encrypts data read from the storage medium or that the bus key is generated by the storage device. However, Utsumi discloses a storage device that encrypts data read from the storage medium and obtains the key from same (Utsumi, paragraph 0053). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention by Lotspiech to relocate the encryption means onto the storage device, as taught by Utsumi. The motivation for this would be to more reliably protect the copyright of the digital contents (Utsumi, paragraph 0020).

Referring to Claim 18:

Lotspiech discloses an apparatus comprising:

a storage device to access a storage medium containing data and a key distribution data block, said storage device including a processing logic (col 5, lines 1-10),

a one-way function and an encryption logic, wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said storage device to compute a media key (col 5, lines 1-5),

said one-way function combines said media key with a nonce received over a data bus from a number generator to produce a bus key (col 5, lines 1-10, 20-25) and

said encryption logic encrypts said data accessed from said storage medium using said bus key prior to transmitting the encrypted data via a data bus to a host device (col 5, lines 5-25).

Lotspiech does not explicitly teach that the one-way function logic and encryption logic are contained within the storage device. However, Utsumi teaches encryption logic contained within a storage device (Utsumi, paragraph 0053). It should be noted that one-way functions are well known in the art as a form of encryption, and that consequently one-way function logic can be construed to be a type of encryption logic. Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention disclosed by Lotspiech such that the one-way function logic and encryption logic presently taught be relocated inside the storage unit. The motivation for this would be to more reliably protect the copyright of the digital contents (Utsumi, paragraph 0020).

Referring to Claim 2:

Lotspiech and Utsumi disclose the limitations of Claim 1 above. Lotspiech further discloses a decryption subsystem coupled to said data bus to, decrypt said encrypted

data received over the data bus using a decryption bus key derived based [1] a portion of the key distribution data block, [2] a device key assigned to said decryption subsystem and [3] the nonce generated by the number generator (col 5, lines 10-20).

Referring to Claim 3:

Lotspiech and Utsumi disclose the limitations of Claim 1 above. Lotspiech further discloses said encryption subsystem comprises:

a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said encryption subsystem to compute a media key (col 5, lines 1-10);

a one-way function to generate the encryption bus key based on the media key and the nonce generated by the number generator (col 5, lines 1-6);

and an encryption logic to encrypt data accessed from said storage medium using said encryption bus key (col 5, lines 1-10).

Referring to Claim 4:

Lotspiech and Utsumi disclose the limitations of Claim 2 above. Lotspiech further discloses said decryption subsystem comprises:

a processing logic to process at least a portion of the key distribution data block read from the storage medium using the at least one device key assigned to said decryption subsystem to compute a media key (col 5, lines 10-20);

a one-way function to generate the decryption bus key based on said media key and the nonce generated by the number generator (col 5, lines 15-20); and

a decryption logic to decrypt data transmitted over the data bus by using said decryption bus key (col 5, lines 18-20).

Referring to Claims 5, 12 and 20:

Lotspiech and Utsumi disclose the limitations of Claims 1, 11 and 18 above. Lotspiech further discloses said data transmitted over the data bus is encrypted using the bus key derived based on the nonce generated by the number generator such that if said data is recorded at the time of transmission, said recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by said encryption subsystem to encrypted said data transmitted over the data bus (col 5, lines 20-35).

Referring to Claims 6, 16 and 26:

Lotspiech and Utsumi disclose the limitations of Claims 2, 11 and 19 above. Lotspiech further discloses said key distribution data block is embodied in the form of a media key block comprising a block of encrypted data (col 4, lines 20-30).

Referring to Claim 7:

Lotspiech and Utsumi disclose the limitations of Claim 2 above. Lotspiech further discloses said encryption subsystem is implemented in a storage device capable of

accessing data from a storage medium and said decryption subsystem is implemented in a host device capable of retrieving data from said storage device (col 5, lines 1-20; Fig. 1).

Referring to Claim 8:

Lotspiech and Utsumi disclose the limitations of Claim 2 above. Lotspiech further discloses said media key computed by the said encryption subsystem will be the same as the media key computed by the decryption subsystem provided that neither the device key assigned to the encryption subsystem nor the device key assigned to the decryption subsystem have been compromised (col 5, lines 10-20).

Referring to Claim 9:

Lotspiech and Utsumi disclose the limitations of Claim 2 above. Lotspiech further discloses wherein said storage medium is selected from digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory magnetic card and optical card (Fig. 1).

Referring to Claim 13:

Lotspiech and Utsumi disclose the limitations of Claim 11 above. Lotspiech further discloses decrypting the encrypted data received over the data bus (col 5, lines 10-20).

Referring to Claim 14:

Lotspiech and Utsumi disclose the limitations of Claim 13 above. Lotspiech further discloses said decrypting the encrypted data received over the data bus comprises:

a host device reading the key distribution data block from the storage medium (col 5, lines 10-20);

the host device processing at least a portion of the key distribution data block using at least one device key to compute a media key (col 5, lines 10-20);

the host device fetching the nonce generated by the number generator (col 5, lines 10-35);

the host device combining said media key with the nonce using a one-way function to generate a bus key (col 5, lines 10-20); and

the host device decrypting said encrypted data received over the data bus using the bus key generated by the host device (col 5, lines 10-20).

Referring to Claim 19:

Lotspiech and Utsumi disclose the limitations of Claim 18 above. Lotspiech further discloses a host device coupled to said storage device via said data bus, said host device including

a processing logic, a one-way function and a decryption logic (col 5, lines 10-20), wherein said processing logic processes at least a portion of said key distribution data block using a device key assigned to said host device to compute a media key (col 5,

lines 10-20), said one-way function combines said media key with said nonce generated by said number generator to produce a bus key and said decryption logic decrypts said encrypted data received over the data bus using said bus key (col 5, lines 10-35).

Referring to Claim 21:

Lotspiech and Utsumi disclose the limitations of Claim 19 above. Lotspiech further discloses said media key computed by the said storage device will be the same as the media key computed by the host device provided that neither the device key assigned to the storage device nor the device key assigned to the host device have been compromised (col 5, lines 10-20).

Referring to Claim 23:

Lotspiech and Utsumi disclose the limitations of Claim 19 above. Lotspiech further discloses said storage device is embodied in the form of a DVD drive and said host device is embodied in the form of either a DVD player or a personal computer (col 1, line 30-35; Fig. 1).

Referring to Claim 24:

Lotspiech and Utsumi disclose the limitations of Claim 19 above. Lotspiech further discloses said storage medium is selected from a digital versatile disc (DVD), CD-ROM, optical disc, magneto-optical disc, flash-based memory, magnetic card and optical card (Fig. 1).

5. Claims 10, 17, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech in view of Utsumi as applied to claims 2, 14, and 19 above, and further in view of Kato et al (U.S. Patent 6,751,321).

Neither Lotspiech nor Utsumi explicitly disclose "said number generator is a random number generator residing within the host device". However, Kato discloses said number generator is a random number generator residing within the host device (col 5, lines 30-50). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Lotspiech such that the "media id" number generator that produces the nonce is a random number generator. One of ordinary skill in the art would have been motivated to do this because it would provide increased security (col 5, lines 47-50).

6. Claims 10, 17, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech in view of Utsumi as applied to claims 2, 14, and 19 above, and further in view of Jakobsson et al. ("A Practical Secure Physical Bit Generator", ©1998 ACM).

Neither Lotspiech nor Utsumi explicitly disclose that "said number generator is a random number generator residing within the host device." However, Jakobsson discloses a method by which a magnetic hard disk, as well as other types of storage devices, can be used to generate a string of random bits (Jakobsson, "Abstract"). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the random number generating method disclosed by Jakobsson

into the invention disclosed by Lotspiech, by using the hard drive residing within the Jakobsson device as a random number generator (Lotspiech, column 3, lines 58-67). One would be motivated to do so because true randomness increases the efficiency of cryptographic operations (Jakobsson, "Introduction", 1st paragraph).

7. Claims 15 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech in view of Utsumi as applied to claim 19 above, and further in view of Nagai et al. (U.S. Pre-Grant Patent Application 2002/0015494).

Regarding claim 15:

Lotspiech and Utsumi disclose the limitations of Claim 13 above. In addition, Utsumi discloses the storage device encrypting said descramble key read from said storage medium with said bus key generated by said storage device and sending said encrypted descramble key to the host device (Utsumi, paragraphs 0009 and 0010).

Neither Lotspiech nor Utsumi explicitly disclose "the host device requesting a descramble key required for descrambling scrambled content from said storage device;

the host device decrypting said encrypted descramble key received from said storage device using said bus key generated by said host device the host device descrambling said decrypted data using said descramble key decrypted by said host device."

Nagai discloses the host device requesting a descramble key required for descrambling scrambled content from said storage device (paragraph 0059);

the host device decrypting said encrypted descramble key received from said storage device using said bus key generated by said host device the host device descrambling said decrypted data using said descramble key decrypted by said host device (paragraphs 0051 and 0059-0060)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the combination of Lotspiech and Utsumi such that the data stored on the storage medium is scrambled. One of ordinary skill in the art would have been motivated to do this because it would provide a higher level of copy protection (paragraphs 0049-0051).

Regarding claim 25:

Neither Lotspiech nor Utsumi explicitly disclose "said storage medium is embodied in the form of a DVD containing scrambled content". However, Nagai discloses said storage medium is embodied in the form of a DVD containing scrambled content (paragraph 0059). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Lotspiech such that the information stored on the medium is scrambled. One of ordinary skill in the art would have been motivated to do this because it would provide a higher level of copy protection (paragraphs 0049-0051).

8. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lotspiech in view of Utsumi as applied to claim 19 above, and further in view of Kawamae et al. (U.S. Patent 6,778,757).

Neither Lotspiech nor Utsumi explicitly disclose "said storage medium is embodied in the form of a DVD containing scrambled content". However, Kawamae discloses a recordable DVD medium that can contain scrambled content (Kawamae, col. 3, line 43 – col. 4, line 3). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a recordable DVD medium, such as DVD+RW, DVD-RW, or DVD-RAM, as the storage medium used in the invention disclosed by Lotspiech. The motivation for this would be to take advantage of the very large capacity of the DVD media (Kawamae, col. 1, lines 21-31).

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:00am - 4:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
6/2/05

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100